Colloquium Brief: Cyber Infrastructure Protection

December 19, 2011 | Dr. Tarek N. Saadawi, COL Louis H. Jordan, Jr

Tagged in: Cyber Security, Colloquium Brief

A partnership between:

U.S. Army War College,

Strategic Studies Institute;

Center of Information Networking and Telecommunications,

Grove School of Engineering;

Colin Powell Center for Public Policy; and

City University of New York, City College

Key Insights:

- There is a relentless struggle taking place in the cyber sphere as government and business spend billions attempting to secure sophisticated network and computer systems.
- Cyber attackers are able to introduce new viruses, worms, and bots capable of defeating many of our efforts.
- It is essential to explore the market for malicious software and cybercrime services in order to understand the price and availability of resources, as well as the relationship between the

price paid for services and the cost experienced by victims of these crimes.

- The emergence of the civilian cyber warrior (and perhaps the physical attack counterpart) is an event that should be carefully taken into account when developing policies and distributing resources across national priorities to protect national critical infrastructures.
- Criminal justice and social education models should be concerned with securing the highly distributed elements of the information networks, extending the effective administration of justice to cybercrime, and embedding security awareness and competence in engineering and common computer practice.
- Three reasons make the state data breach disclosure laws, recently enacted in most states in the United States, of interest: the rapid policy growth; this is the first instantiation of informational regulation for information security; and the importance of these laws to identity theft and privacy, all of which are areas of growing concern.
- The diverse and sophisticated threats posed by hackers and malicious software writers require significant investigation by both the technical and social sciences to understand the various forces that affect participation in these activities.

Introduction.

A two-day colloquium titled Cyber Security Infrastructure Protection was conducted on June 8-9, 2011, by the Center of Information Networking and Telecommunications (CINT) at the Grove School of Engineering, the Colin Powell Center for Public Policy, both at the City University of New York, City College (CCNY), and the Strategic Studies Institute (SSI) at the U.S. Army War College. The colloquium brought together government, business, and academic leaders to assess the vulnerability of our cyber infrastructure and provide strategic policy direction for the protection of that infrastructure.

There is a relentless struggle taking place in the cyber sphere as government and business spend billions attempting to secure sophisticated network and computer systems. Cyber attackers are able to introduce new viruses, worms, and bots capable of defeating many of these efforts. The U.S. Government has set a goal of modernizing the nation's energy grid. A cyber attack on our energy grid could cutoff service to large areas of the country. Government, business, and academia must therefore work together to understand the threat and develop various modes of fighting cyber attacks, and to establish and enhance a framework for deep analysis for this multidimensional issue.

The cyber infrastructure protection conference for Academic year 2010-11 focused on the strategic and policy directions and how these policy directions should cope with fast-paced technological evolution. Topics addressed by the conference attempted to answer some of these questions: How serious is the cyber-threat? What technical and policy-based approaches are best suited to securing Telecommunications Networks and Information Systems Infrastructure security? What role will government and the private sector play in homeland defense against cyber-attack on critical civilian infrastructure, financial, and logistical systems? What legal impediments exist to efforts to defend the nation against cyber-attacks, especially in the realm of preventive, preemptive, and retaliatory actions?

The Colloquium was organized into three main sessions. Session 1 discussed the economics and social aspects of cyber security covering the economics of malicious software and stolen data markets as well as the emergence of the civilian cyber warrior. Session 2 dealt with laws and cyber crime covering social and justice models for enhanced cyber security, and provided an institutional and developmental analysis of data breach disclosure laws. It also provided solutions for critical infrastructure that protect civil liberties, enhanced security, and explored the utility of open source data. Session 3 presented the technical aspects of the cyber infrastructure and presented monitoring for internet service provider (ISP) grade threats, as well as the challenges associated with cyber issues.

Session 1: Economics and Social Aspects of Cyber Security.

The first two papers provided a framework for the economics and social aspects of cyber security. In the first paper, Thomas Holt explained how hackers are utilizing data from a sample of active publicly accessible web forums that traffic in malware and personal information. To explore and expand our understanding of the economics of cybercrime in general, this session utilized a qualitative analysis of a series of threads from publicly accessible Russian web forums. These forums facilitate the creation, sale, and exchange of malware and cybercrime services. The findings explore the resources available within this marketplace and the costs related to different services and tools. Using this economic data coupled with loss metrics from various studies, this analysis considers the prospective economic impact of cybercrime campaigns against civilian and business targets. The findings provide insight into the market dynamics of cybercrime and the utility of various malware and attack services in the hacker community.

In summary, it can be said that this presentation explored the market for malicious software and cybercrime services in order to understand the price and availability of resources, as well as the relationship between the price paid for services and the cost experienced by victims of these crimes.

The paper by Max Kilger focused on the civilian cyber warrior—that poses perhaps the most significant emerging threat to domestic and foreign critical infrastructures. The presentation started by providing some basic background for a schema that outlines six motivational factors which are hypothesized to encourage malicious online behaviors.

The key concept is that perhaps for the first time in history, a regular civilian can effectively attack a nation-state—in this case through a cyber attack on some component of that nation-state's critical infrastructure. In this use, effective means that the attack can cause significant widespread damage, has a reasonably high probability of success, and a low probability of the perpetrator being apprehended. One of the first things that one might want to investigate in the chain of actions for a cyber attack is the initial starting point where individuals begin thinking about and rehearsing in their minds the nature, method, and target for the attack. Perhaps the key point of the historical and social significance of the emergence of civilian cyber warriors can be found in the social psychological significance of the event. The reassessment of the usual assumptions of the inequalities of the levels of power between nation-states and citizens establishes new relationships between institutions of society, government, and individuals.

After an initial examination of the severity of physical and cyber attacks where survey respondents feel it is appropriate to launch an attack against a foreign country, the survey results provide both good and bad news. On the one hand, the vast majority of respondents indicated that they only engage in attacks that have minor or no consequences to the targeted foreign country. On the other hand however, there were a nontrivial number of respondents who personally advocate the use of physical and cyber attacks against a foreign country even though those attacks may have some moderate to very serious consequences. There is some comfort to be had in the fact that expressing intentions to commit terrorist acts is only the first link in the behavioral chain from ideation to the actual execution of an attack. Bearing in mind that this is a scenario-based situation, even a small number of individuals who would consider some of the most serious acts is a troubling consideration. This suggests that the emergence of the civilian cyber warrior (and perhaps the physical attack counterpart) is an event that should be carefully taken

into account when developing policies and distributing resources across national priorities to protect national critical infrastructures. Knowing your enemy can be a key element in gaining a comprehensive perspective on attacks against online targets.

Session 2: Law and Cyber Crime.

The law and cyber crime were explored in Session 2 of the Colloquium. The presentation by Michael M. Losavio argued that to change the game in cyber security, we should consider criminal justice and social education models to secure the highly distributed elements of the information network, extend the effective administration of justice to cybercrime, and embed security awareness and competence in engineering and common computer practice. Safety and security require more than technical protections and police response. They need a critical blend of those elements with individual practice and social norms. Social norms matched with formal institutions enhance public safety, including in the cyber realm. Informal and formal modes of controlling and limiting deviant behavior are essential for effective security.

The presentation suggested that routine activity theory/opportunity theory and displacement theory—frameworks for analyzing crime in communities—are ways to conceptualize and pattern the benefits of informal social control on cyber security. Routing Activity Theory (RAT) suggests that for cyber security the analysis should equally consider the availability of suitable targets, a presence or lack of suitable guardians, and an increase or decrease in the number of motivated offenders, particularly those seeking financial gain or state advantage. Online social networks themselves suggest opportunities for the examination of RAT-based security promotion. Facebook, MySpace, and LiveJournal are online social networks that can be used to promote cyber security both inside and outside of their domains. RAT can also be applied to criminal activity involving computing systems. Criminological principles of cyber security also relate to the use of criminal profiling and behavioral analysis. The reactive use of these techniques, much like the use of technical digital forensics in network settings, serves to focus an investigation and response in particular areas and on particular individuals. Proactive use of profiling is used to deter or prevent crime, such as drug courier profiling.

In the second presentation, Melissa Dark considered the state data breach disclosure laws recently enacted in most states in the United States. Three reasons make the state data breach disclosure laws of interest: the rapid policy growth; this is the first instantiation of informational

regulation for information security; and the importance of these laws to identity theft and privacy, all of which are areas of growing concern.

Technological advancements are considerably changing the information security and privacy landscape. Yet, these policies are blunt instruments, which are not well-suited for the careful excision of these ills. Some advocates who call for the modfication of existing laws assert that the outcome of data breach disclosure should be to motivate large-scale reporting so that data breaches and trends can be aggregated, which allows a more purposeful and defensive use of incident data.

The third presentation by Joshua Gruenspecht addressed the problems of identity determination, which raises some of the most complicated unresolved issues in cyber security. Industry and government are pursuing a number of approaches to better identify communicants in order to secure information and other assets. As part of this process, some policymakers have suggested that fundamental changes to the way in which the Internet transmits identity information may be required. Authentication is "the process of establishing an understood level of confidence that an identifier refers to a particular individual or identity." Authentication often involves an exchange of information before some other transaction is completed in order to ensure —to the extent necessary for the transaction at hand—that the sender of a stream of traffic is who he or she claims to be or otherwise has the attributes required to engage in the given transaction. Attribution is the analysis of information associated with a transaction or series of transactions to try to determine the identity of a sender of a stream of traffic. Information collection and analysis is the focus of attribution. This presentation focused on authentication and attribution, two other issues are closely related to identity and are critical elements of any secure system: authorization and auditing. The presentation considered these problems and concluded that authentication-oriented solutions are more likely to provide significant security benefits and less likely to produce undesirable economic and civil liberties consequences.

The presentation by George W. Burruss focused on the value of open reporting for malware creation and distribution. He considered how this information may be combined with other measures to explore the country-level economic, technological, and social forces that affect the likelihood of malware creation. The speaker proposed that online repositories containing data on malicious software can be valuable to study the macro-level correlates of malware creation. The data for the dependent variable used for this study came from an open source malware repository

where individuals could post information obtained on malicious software. The data for the independent variables were derived from the *CIA World FactBook* and from Freedom House, a nongovernmental agency that collects annual data on political freedom around the globe.

The speaker concluded that the diverse and sophisticated threats posed by hackers and malicious software writers require significant investigation by both the technical and social sciences to understand the various forces that affect participation in these activities. He suggested that there is a strong need for greater qualitative and quantitative examinations of hacker communities around the world. Research on hacker subcultures in the United States, China, and Russia suggests that there are norms, justifications, and beliefs that drive individual action.

Session 3: Cyber Infrastructure.

Abhrajit Ghosh presented a comprehensive view of network security in light of several years of research conducted at Telcordia, focusing mainly on the problem of monitoring large scale networks for malicious activity. The goal of the system that was developed is to detect various types of network traffic anomalies that could be caused by distributed denial-of-service (DDoS) attacks, spamming, IP address spoofing, and botnet activities. Currently three types of anomaly detectors are provided to collect data and generate alerts: (a) Volume Anomaly Detectors; (b) Source Anomaly Detectors; and, (c) Profile Anomaly Detectors. The goal of source anomaly detectors is to identify instances of source IP address spoofing in observed flows. In this case, data for the monitored ISP is acquired via NetFlow/sFlow data feeds from three flow agents. The profile anomaly detectors are intended to detect any behavioral anomalies pertaining to hosts within the monitored network. One profile anomaly detector that is currently part of the system is used to identify potential spammers which use flow data and spammer blacklists. The Telcordia system incorporates an efficient real-time volume anomaly detector that is designed to give early warning of observed volume anomalies. The volume anomaly detector operates by considering a near term moving window of flow records when computing traffic volumes for a destination address. The system incorporates a correlation engine that is used to compare the relationship of alerts that are generated by the different types of anomaly detectors. A significant issue with many anomaly detection based approaches is their potentially high false-positive rate. The correlation engine component is designed to reduce the possibility of generating false positives. Finally, it is suggested that the use of an alert correlation component can be very valuable to a network operator who would be is interested in lowering false-positive rates.

The goal of the presentation by Stuart Starr was to explore the state-of-the-art in our ability to assess cyber issues. To illuminate this issue, he presented a tentative decomposition of the problem into manageable subsets. Using that decomposition, the speaker identified potential cyber policy issues that warrant further analyses and he identified and illustrated sample Measures of Merit (MoMs). Subsequently, Starr characterized some of the more promising existing cyber assessment capabilities that the community is currently employing and he provided an identification of several cyber assessment capabilities that will be needed to support future cyber policy assessments. The presentation concluded with a brief identification of high priority cyber assessment efforts that warrant further action.

*****

*****

More information on the Strategic Studies Institute's programs may be found on the Institute's homepage at *www.StrategicStudiesInstitute.army.mil.*